CLAIMS

1. Method for checking the signature of a message, the message, signature and a certificate having been sent by a signer having a public key to a recipient having a message storage device (11), characterised in that it comprises stages according to which :

- the message, signature and certificate are loaded from the storage device (11) onto a protected device (21) connected to said storage device (11) of the recipient,
- the certificate in the protected device (21) is checked by means of a public key of a reliable third party associated with said certificate, and at least one data element of the result of checking is transmitted to a display device (30) connected directly to the protected device (21),
- the result data element is checked on the display device (30),
- when the certificate is verified, a reduction of the message is calculated in the protected device (21) and the message is recopied onto the display device (30) during the reduction operation,
- the signature with the public key of the signer are decrypted in said protected device (21),
- the signature decrypted is compared with the carried out reduction, and
- according to the result of this comparison, a message is sent from the protected device (21) to the display device (30) indicating that the signature conforms/does not conform to the message or the public key of the signer put forward.

2. Checking method according to claim 1, characterised in that during loading of the certificate the

public key of the reliable third party is loaded.

3. Checking method according to claim 1 or 2, characterised in that said protected device (21) is constituted by a microprocessor card placed in a box (22) connected firstly to said storage device (11), and secondly to said display device (30).

4. Checking method according to any one of the preceding claims, characterised in that said display device (30) is a printer, a screen or a filing device.

5. Checking method according to any one of the preceding claims, characterised in that said protected device (21) sends said display device (30) result data of said certificate, such as the date of validity of the certificate.

6. Checking method according to any one of the preceding claims, characterised in that the protected device (21) comprises firstly a commands/data interface circuit (221) embodying a link with the storage device (11), and secondly a display interface circuit (223) embodying a link with the display device (30), said circuits being physically independent.